Pre-Processing Power Traces to Defeat Random Clocking Countermeasures

Philip Hodgers, Neil Hanley, Maire O'Neill
Centre for Secure Information Technologies (CSIT)
ECIT, Queen's University Belfast
Belfast BT3 9DT, United Kingdom
p.hodgers@qub.ac.uk, n.hanley@qub.ac.uk, m.oneill@ecit.qub.ac.uk

***Abstract*—We describe a pre-processing correlation attack on an FPGA implementation of AES, protected with a random clocking countermeasure that exhibits complex variations in both the location and amplitude of the power consumption patterns of the AES rounds. It is demonstrated that the merged round patterns can be pre-processed to identify and extract the individual round amplitudes, enabling a successful power analysis attack. We show that the requirement of the random clocking countermeasure to provide a varying execution time between processing rounds can be exploited to select a sub-set of data where sufficient current decay has occurred, further improving the attack. In comparison with the countermeasure's estimated security of 3 million traces from an integration attack, we show that through application of our proposed techniques that the countermeasure can now be broken with as few as 13k traces.**

Keywords—power analysis attacks; random clocking; FPGA;

I. INTRODUCTION

A cryptographic device consumes the majority of its current during the dynamic switching activity of the CMOS technology upon which it is built. Like any other computationally intensive operation, cryptography requires a significant amount of processing (switching) activity and therefore consumes measurable amounts of power, which can be acquired with low-cost equipment such as oscilloscopes, probes and amplifiers [6]. Power based side-channel attacks (SCA) exploit the unintended leakage of key-dependent information during cryptographic processing to reveal the secret encryption key. The first power analysis attack of differential power analysis (DPA), was introduced in [2] and extended with electro-magnetic (EM) analysis in [3] and [4]. Correlation power analysis (CPA) [5], which uses Pearson's sample correlation coefficient to compare a set of modelled versus measured power values, has been shown to be an extremely effective and robust method to recover keys from many different platforms. Subsequently there have been many proposals to prevent SCA by breaking the statistical link between the instantaneous power consumption and the key-dependent data or operation being processed. In this work we examine a proposal for a random clocking countermeasure (CM) for FPGAs as presented in [7] and [8].

In comparison to lower-frequency cryptographic devices, such as smart cards and micro-controllers, which often complete individual processor instructions in a clock frequency range of 2 MHz to 12 MHz, FPGA's can execute the combinatorial logic of a round of AES in a single 1/24 MHz period [10]. At these higher clock frequencies we can observe changes in the power consumption patterns such as the merging of the previously distinct rounds of AES [9]. This merging is produced when the CMOS circuitry has not had time to fully discharge its capacitive store of current before starting the next round of the algorithm, hence re-charging of the circuitry commences. The effect is exploited by the CM under consideration to incorporate larger variations in the round peak amplitudes, alongside the randomization of the temporal positioning of the AES rounds.

Our contribution is the development of a charge and decay modelling approach that identifies which features of the protected power consumption patterns relate to the individual rounds of the algorithm. We also exploit the necessity for the countermeasure to exhibit variation in execution time between processing rounds to identify a subset of traces that improves the attack further. We show that the countermeasure's estimated security requirement of 3 million traces [7], to break with an integration attack, can be reduced to around 13k traces using our approach.

The remainder of this paper is organized as follows. In Section II the random clocking countermeasure and its effect on power consumption traces is examined. We then look at the applicability of existing attack methods. In Section III we introduce our charge/decay modelling attack, with experimental results presented in Section IV and conclusions in Section V.

II. BACKGROUND

A. Random Clocking Countermeasure

In order for a distinguisher such as CPA [5] to operate successfully, it requires that the power consumption waveforms are sufficiently aligned with respect to one-another, such that the targeted operation in the encryption algorithm occurs at the same point in time across each of the sampled traces. Misalignments may be unintentionally introduced due to experimental error, such as through lack of a suitable triggering source, by processor interrupts, or through intentional countermeasures such as the random process interrupts proposed in [11], clock skipping in [1], or the random clocking CM of [7] and [8] considered here.

The use of a random clock is an attractive countermeasure due to its low cost with regards area, power consumption and timing penalties, as well as providing for significantly increased resistance against DPA attacks. The randomization of the clock desynchronizes the point in time where the targeted operation is

processed, as well as affecting the amplitude of the trace, which is also dependent on the frequency, as shown in (1).

$$P_{dyn} = f \cdot C_L \cdot \alpha \cdot {V_{DD}}^2 \quad (1)$$

Here the dynamic power consumption P_{dyn} is a function of the clock frequency f, the capacitive load C_L, the switching activity α, and the supply voltage of the circuit V_{DD}. The switching activity α refers to the number of transistors that change state, which itself is dependent on the data and operations being performed. A more detailed overview of power traces, in the context of SCA, can be found in [6].

The method of implementing random clocking in this work is the same as suggested in [7] and [8] and is shown in Figure 1, where an input clock CLK_{in} is fed through digital clock managers DCM, which generate jitter free clocks at various phase-selectable PS outputs. A random number generator RNG is used to constantly change the selected clock by randomly selecting one of many phase-offset outputs from the DCM. Dedicated clock buffers are available to route the selected DCM outputs to the global and local clock distribution networks. Note that extra delays are introduced due to the operation of the clock multiplexors as explained in [7].

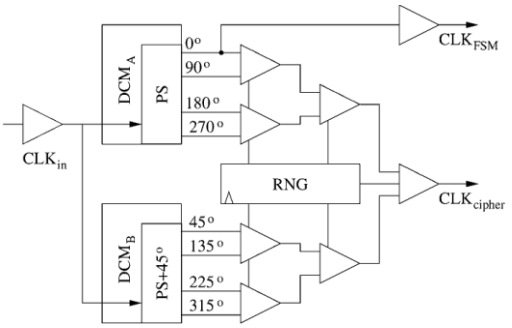

Figure 1: The random clocking countermeasure of [7].

The net result of this random clocking countermeasure can be observed in Figure 2, where two power traces of the protected implementation of AES are shown. It is evident that the traces have differing patterns, with variation in peak amplitudes and overall execution times. Note also that some of the rounds have become merged together, making it more difficult to separate and identify the individual processing rounds. This merging also causes a cumulative charging of the power consumption pattern.

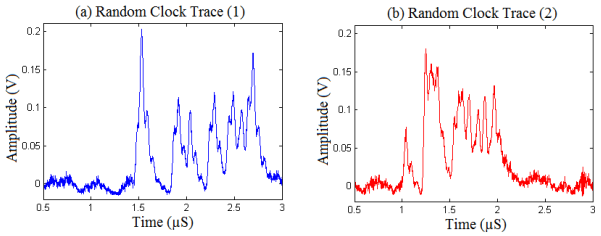

Figure 2: Power consumption traces of the implemented CM.

B. *Existing Approaches to Overcome Random Clocking*

There are some general pre-processing techniques that may be applied to trace data to help improve a correlation attack. An integrating window or comb function can be used to select a number of samples that are summed together to represent the net effect of a region of power consumption. This is essentially an averaging technique and therefore introduces a loss of precision due to the difference in the variances of the summed elements. The correlation coefficient value has been shown to diminish by $\sqrt{l}$, where l is the length of the integrating window [6]. The integration approach is therefore best suited to smaller regions of misalignment.

Another approach is to perform the attack in the frequency domain [12], however discrete Fourier transform (DFT) based approaches operate best when the windowing region can be minimized around the region of interest, as examined in [13]. Phase-only correlation was suggested in [14], where the differences in phase values are used as a realignment vector. The data is then converted back into the time domain for the side-channel analysis. The technique is best suited to high resolution realignment, such as overcoming oscilloscope acquisition errors.

Some specific attacks against random clocking CMs have been proposed. The wavelet continuous transform of [15] introduced a time-frequency analysis, applying it to the Data Encryption Standard (DES) power traces of a smart card running a random clocking CM. A simulated annealing procedure was applied to the traces to assist with stretching and compressing the individual round patterns to match a chosen reference trace. For our randomly merged trace patterns of Figure 2, only a small proportion of the trace population would have similar merging patterns to a randomly chosen reference, with annealing therefore potentially distorting the waveforms significantly.

The deconvolution of signals was investigated in [16] using a smart card with a randomly varying clock between 8 MHz and 12 MHz. The approach required the development of a comb function to define the inter-round boundaries. In the context of the randomly merging round patterns of Figure 2, a chosen comb pattern will only select the appropriate round peaks for the reference upon which the comb is developed. Only a small number of the other traces could be expected to match this comb.

An elastic alignment method was proposed in [17] with an optimized variant termed the rapid alignment method in [18]. The technique also uses a reference trace, to which the other traces are dynamically stretched or compressed. The approach is similarly limited, in the context of merged rounds, as discussed. We therefore seek an approach that will overcome these issues.

III. Charge and Decay Profiling

A. *Identifying the Rounds of AES*

The waveform patterns of Figure 2 consist of periods of processing activity that generate a steep rise in power consumption, when a round of AES is being processed, followed by periods of inactivity that are characterized by charge decay. While it is a relatively straightforward task to identify single rounds of processing, in isolation, it becomes a more difficult task to interpret patterns where the rounds are processed in close proximity and thus a merging of the rounds occurs.

It was shown in [6] that the peak amplitude of a processing round is often sufficient to perform SCA. Therefore the aim is to identify the representative peak values of each round in the protected waveforms. As a first step we can simplify the

waveform pattern to remove some of the high frequency noise. A 120 MHz digital finite impulse response (FIR) low-pass filter was applied to a power trace generated by the countermeasure, with the resulting trace shown in Figure 3(a). The trace has been zoomed-in to the region of processing for the purposes of clarity.

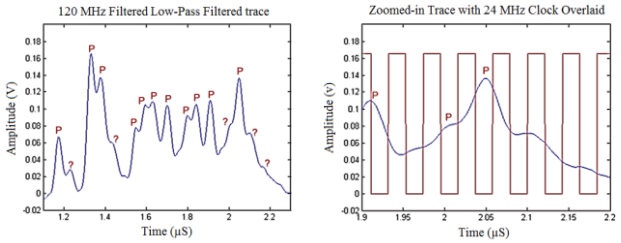

Figure 3: (a) Visually extracting round information.
(b) Eliminating uncertain rounds via minimum separation metrics.

A cursory visual inspection of Figure 3(a) enables several processing rounds to be identified, and these are annotated with a P. However, there remain a few features which are not yet certain, highlighted with question marks. When the first processing peak P occurs in Figure 3(a), it is followed by a smaller decaying peak. Similarly, after the third P, and after the last P, a similar pattern occurs. In each case a small amount of re-charging occurs, before continuing to decay. Referring back to the design of Figure 1, the countermeasure receives an input clock, which in the case of our SASEBO-G [10] has been set to 24 MHz, and generates a randomly delayed phased-offset clock to feed the encryption core. The rest of the FPGA is still operating off the main 24 MHz system clock, therefore these decay features do not relate directly to processing the encryption round, but rather to other power consumption activities linked to the global clock tree and therefore may be considered as clock-tree artefacts to be ignored.

An unknown feature in Figure 3(a) is the question mark just before the final P. It would appear that this is a processing operation, immediately followed by another operation, burying that round's peak somewhere in the merged round shape. In order to determine whether there are merged rounds, it is useful to measure the length of time taken to process the two features. A useful comparison method is an overlaid clock trace, since this provides a pattern with regular spacing and can eliminate peak candidates that are too close together. Figure 3(b) shows the zoomed-in section of the last round of Figure 3(a), overlaid with a 24 MHz clock. Since the separation distance in 3(b) is greater than one 1/24 MHz clock period, it is deemed to be a separate processing activity and is marked with a P. If it were less than one clock period (the minimum possible) it would have been interpreted as part of the final round itself. Note that in our implementation we have two peaks relating to the initialization of the cipher, with the following 10 peaks corresponding to the 10 rounds of AES.

IV. Experimental Results

A. Attacking the Random Clocking Countermeasure

A SASEBO-G [10] with VIRTEX-II FPGA was loaded with an implementation of AES and the random clocking CM under consideration. A set of 500k traces were acquired and filtered with a 120 MHz FIR filter to remove high frequency noise. A max/min algorithm was then developed to parse through each power trace to identify all maxima and minima, as per Figure 4.

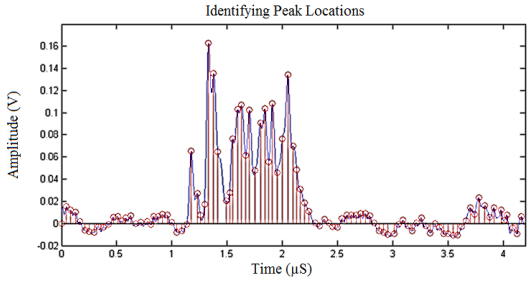

Figure 4: Power trace with all maxima and minima identified.

The maxima were then evaluated pairwise consecutively to determine if a large charging (round processing) feature was present. A second pass through the peaks then considered the amount of decay relative to the neighboring value to determine whether the peak should be considered as a processing round, or as a clock-tree artefact. The threshold for this was arbitrarily determined to be 30% decay by inspection of several traces. This value is implementation specific and would need to be determined for any given data set. The merged features were then detected using the described minimum separation metric. The resulting peak detections are shown in Figure 5, which has again been zoomed-in for clarity.

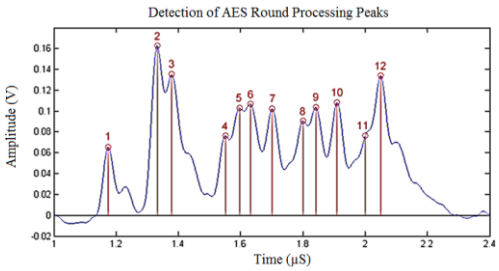

Figure 5: Power trace with AES processing rounds identified.

As mentioned, the threshold for clock decay was arbitrarily chosen and is not ideal for all traces. Consequently, when pre-processed with the above algorithm, around 60% of the traces conformed and generated the required 12 peak pattern. Those traces that did not conform were ignored. A CPA attack was performed on the 500k trace set, targeting a byte of the register transition from the final round to the ciphertext. The attack was successful after approximately 30k traces, correctly identifying the target key byte value with a distinctly higher correlation value, as shown in Figure 6(a). For comparison, and to confirm that there was no inherent leakage making the attack successful, an integration attack was also performed. As shown in Figure 6(b), the attack was unsuccessful with a low correlation value.

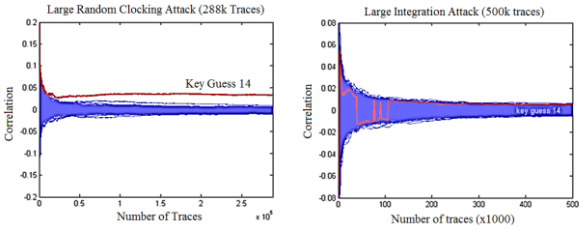

Figure 6: (a) Successful attack (b) Failed integration attack.

B. *Improving the attack with a Round Separation Metric*

Since the random clocking CM has to provide enough variation between the times of round executions to sufficiently alter the shape of the waveforms in a random manner, the distance between the final two rounds of the algorithm will also vary. These variations will reside somewhere within the range of the extremes from where no separation is present, to the case where a large enough delay is present that the prior round has had time to fully decay to background levels. If the data set used for the successful correlation attack is now parsed again, but this time to only select traces where the penultimate round has had sufficient time to decay, then the randomized cumulative charging effect can also be minimized, as illustrated in Figure 7.

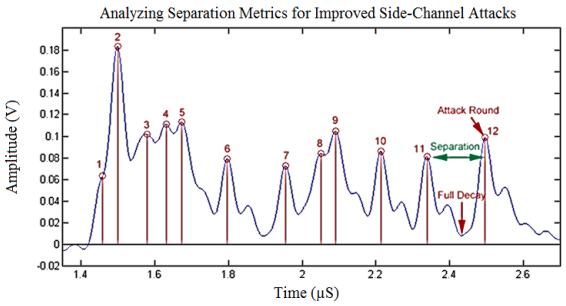

Figure 7: Analyzing the separation metric between the final rounds.

By progressively increasing the separation distance in the partitioning of the data, we can find the optimal distance that requires the fewest overall traces. It is apparent in Table 1 that the optimal separation distance is approximately 4 clock periods, leading to a successful attack with only 13.4 k traces. It might be expected that the largest separations would yield the best results, however, there are a lower number of traces available from those sets, since it requires more original traces to be acquired to generate these more extreme trace sets.

Clock Periods	Traces in Set	Min Required for Attack	Factor for Total Traces	Total Traces
NA	288 k	30 k	1.74	52.2 k
> 2	113 k	8 k	4.42	35.4 k
> 3	63 k	8 k	7.84	63.0 k
> 4	28 k	750	17.86	13.4 k
> 5	16 k	500	31.25	15.6 k
> 6	6 k	500	73.33	36.7 k

Table 1: Analyzing the separation distance between the final rounds. Clock distance > 4 gives the best result, requiring only 13.4 k total traces for success.

V. CONCLUSION

A new pattern analysis attack against a high frequency random clocking CM has been introduced, modelling the rise and fall of power consumption of AES round processing operations, overcoming both the temporal shifting and cumulative charging characteristics of [10] and [11]. While the attack parameters are specific to the data set under examination, the method can be used to provide a simple characterization of the power consumption trace patterns for other devices. The attack could be optimized further to better model the countermeasure and reduce the number of discarded traces (approximately 40% in the demonstrated approach). However, this customization effort needs to be traded against the ease with which further additional traces may be gathered. This work reinforces the view that the random clocking countermeasure should not be relied upon in isolation for protection from power attacks. Rather, it should be coupled with additional countermeasures such as dummy operations and masking.

REFERENCES

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis Method and Apparatus," issued September 8th 2009, US Patent 7,587,044.

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Advances in Cryptology CRYPTO 1999, ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in Cryptographic Hardware and Embedded Systems CHES 2001, ser. Lecture Notes in Computer Science, Cetin Kaya Koc¸, D. Naccache, and C. Paar, Eds., vol. 2162. Springer, 2001, pp. 251–261.

[4] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards," in Smart Card Programming and Security — E-Smart 2001, ser. Lecture Notes in Computer Science, I. Attali and T. P. Jensen, Eds., vol. 2140. Springer Verlag, 2001, pp. 200–210.

[5] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in Cryptographic Hardware and Embedded Systems — CHES 2004, ser. Lecture Notes in Computer Science, M. Joye and J.-J. Quisquater, Eds., vol. 3156. Springer-Verlag, 2004, pp. 16–29.

[6] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer-Verlag, 2007.

[7] T. G¨uneysu and A. Moradi, "Generic Side-Channel Countermeasures for Reconfigurable Devices," in Cryptographic Hardware and Embedded Systems — CHES 2011, ser. Lecture Notes in Computer Science, B. Preneel and T. Takagi, Eds., vol. 6917. Springer-Verlag, 2011, pp. 33–48.

[8] Y. Zafar and D. Har, "A Novel Countermeasure Enhancing Side Channel Immunity in FPGAs," in Advances in Electronics and Micro-electronics— ENICS '08. IEEE, 2008, pp. 132–137.

[9] NIST, "FIPS-197: Advanced Encryption Standard (AES)," National Institute of Standards and Technology publication, 2001, http://www.nist.gov/publication-portal.cfm.

[10] Research Center for Information Security, "Side-channel Attack Standard Evaluation Board (SASEBO)," http://www.risec.aist.go.jp/project/sasebo

[11] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential Power Analysis in the Presence of Hardware Countermeasures," in Cryptographi Hardware and Embedded Systems — CHES 2000, ser. Lecture Notes in Computer Science, C. Paar and C¸ etin Kaya Koc¸, Eds., vol. 1965. Springer-Verlag, 2000, pp. 252–263.

[12] C. H. Gebotys, S. Ho, and C. C. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," in Cryptographic Hardware and Embedded Systems CHES 2005, ser. Lecture Notes in Computer Science, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer, 2005, pp. 250–264.

[13] P. Hodgers, K. Boey, and M. O'Neill, "Variable window power spectral density attack," in International Workshop on Information Forensics and Security — WIFS 2011. IEEE, 2011, pp. 1–6.

[14] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching," in Cryptographic Hardware and Embedded Systems — CHES 2006, ser. Lecture Notes in Computer Science, L. Goubin and M. Matsui, Eds., vol. 4249. Springer-Verlag, 2006, pp. 187–200.R

[15] X. Charvet and H. Pelletier, "Improving the DPA attack using Wavelet transform,", 2005, nIST Physical Security Testing Workshop.

[16] M. Kafi, S. Guilley, S. Marcello, and D. Naccache, "Deconvolving Protected Signals," in Conference on Availability, Reliability and Security — ARES 2009. IEEE Computer Society, 2009, pp. 687–694.

[17] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving Differential Power Analysis by Elastic Alignment," in Topics in Cryptology — CT-RSA 2011, ser. Lecture Notes in Computer Science, A. Kiayias, Ed., vol. 6558. Springer-Verlag, 2011, pp. 104–119.

[18] R. A. Muijrers, J. G. J. van Woudenberg, and L. Batina, "RAM: Rapid Alignment Method," in International Conference on Smart Card Research and Advanced Applications — CARDIS 2011, ser. Lecture Notes in Computer Science, E. Prouff, Ed., vol. 7079. Springer, 2011, pp. 266–282.